

Notice of References Cited	Application/Control No. 10/048,216		Applicant(s)/Patent Under Reexamination CORON ET AL.	
	Examiner David G. Cervetti		Art Unit 2136	Page 1 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,600,725	02-1997	Rueppel et al.	380/30
	B	US-4,991,210	02-1991	Chaum, David	380/30
	C	US-4,996,711	02-1991	Chaum, David L.	380/30
	D	US-5,146,500	09-1992	Maurer, Ueli	380/30
	E	US-5,199,070	03-1993	Matsuzaki et al.	380/30
	F	US-5,299,262	03-1994	Brickell et al.	380/28
	G	US-5,299,263	03-1994	Beller et al.	380/30
	H	US-5,347,581	09-1994	Naccache et al.	380/30
	I	US-5,406,628	04-1995	Beller et al.	380/30
	J	US-5,442,707	08-1995	Miyaji et al.	380/30
	K	US-5,790,675	08-1998	Patarin, Jacques	713/180
	L	US-6,154,841	11-2000	Oishi, Kazuomi	713/180
	M	US-6,243,467	06-2001	Reiter et al.	380/30

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)			
	U	ElGamal, Taher, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, July 1985, IEEE, pp. 469-472.			
	V	Demytko, N., A New Elliptic Curve Based Analogue of RSA, 1994, Springer-Verlag, pp 40-49.			
	W	Koblitz, Neal, Elliptic Curve Cryptosystems, January 1987, Mathematics of Computation, vol 48, number 177, pp 203-209.			
	X	Bellare, Mihir, and Phillip Rogaway, PSS: Provably Secure Encoding Method for Digital Signatures, August 1998, IEEE.			

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 10/048,216		Applicant(s)/Patent Under Reexamination CORON ET AL.	
	Examiner David G. Cervetti		Art Unit 2136	Page 2 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,252,959	06-2001	Paar et al.	380/28
	B	US-6,279,110	08-2001	Johnson et al.	713/180
	C	US-6,298,137	10-2001	Hoffstein et al.	380/30
	D	US-6,697,946	02-2004	Miyaji, Atsuko	713/180
	E	US-6,785,813	08-2004	Vanstone et al.	713/171
	F	US-6,122,736	09-2000	Vanstone et al.	713/169
	G	US-6,105,134	08-2000	Pinder et al.	713/170
	H	US-6,081,598	06-2000	Dai, Wei	380/28
	I	US-6,081,597	06-2000	Hoffstein et al.	380/28
	J	US-6,044,463	03-2000	Kanda et al.	713/168
	K	US-6,038,316	03-2000	Dwork et al.	705/51
	L	US-5,987,138	11-1999	Gilbert et al.	380/30
	M	US-5,987,131	11-1999	Clapp, Craig S. K.	713/171

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Bellare, Mihir, and Phillip Rogaway, The Exact Security of Digital Signatures - How to Sign with RSA and Rabin, March 1996, Springer-Verlag.
	V	KCDSA task Force Team, The Korean Certificate-based Digital Signature Algorithm, August 1998, IEEE.
	W	Nyberg, Kaisa, and Rainer Rueppel, Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem, 1998, Springer-Verlag, pp 182-193.
	X	Atsuko Miyaji, A Message Recovery Signature Scheme Equivalent to DSA over Elliptic Curves, 1996, Springer-Verlag, Lecture Notes in Computer Science, Volume 1163, pp 1-14.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 10/048,216	Applicant(s)/Patent Under Reexamination CORON ET AL.	
	Examiner David G. Cervetti	Art Unit 2136	Page 3 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,966,445	10-1999	Park et al.	713/180
	B	US-5,933,504	08-1999	Vanstone et al.	380/30
	C	US-5,889,865	03-1999	Vanstone et al.	713/171
	D	US-6,563,928	05-2003	Vanstone et al.	380/30
	E	US-6,404,890	06-2002	Lenstra, Arjen K.	380/268
	F	US-6,154,541	11-2000	Zhang, Jinglong F	380/30
	G	US-6,212,637	04-2001	Ohta et al.	380/30
	H	US-5,724,425	03-1998	Chang et al.	380/30
	I	US-6,263,081	07-2001	Miyaji et al.	380/28
	J	US-4,995,082	02-1991	Schnorr, Claus P.	713/169
	K	US-6,510,518	01-2003	Jaffe et al.	713/168
	L	US-6,816,965	11-2004	Moore et al.	713/158
	M	US-5,910,989	06-1999	Naccache, David	713/173

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Burton S. Kaliski Jr., Emerging Standards for Public-Key Cryptography, Jan 1999, Springer-Verlag, Lecture Notes in Computer Science, Volume 1561, Page 87.
	V	Menezes et al., Handbook of Applied Cryptography, 1996, CRC Press, pp 425-488, 635-661.
	W	Naccache, David and Jacques Stern, A New Public Key Cryptosystem Based on Higher Residues, November 1998, ACM, Proceedings of the 5th ACM conference on Computer and Communications Security, pp 59-66.
	X	Pointcheval, David and Jacques Stern, New blind signatures equivalent to factorization, April 1997, ACM, Proceedings of the 4th ACM conference on Computer and Communications Security, pp 92-99.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 10/048,216	Applicant(s)/Patent Under Reexamination CORON ET AL.	
	Examiner David G. Cervetti	Art Unit 2136	Page 4 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,960,085	09-1999	de la Huerga, Carlos	340/5.61
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.